УДК 338:658.5

Р.Ю.Клим
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ЗАСТОСУВАННЯ ОБМАННИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В ЛОКАЛЬНІЙ ІНФОРМАЦІЙНІЙ МЕРЕЖІ

R.Y. Klym

APPLICATION OF FALSE INFORMATION PROTECTION SYSTEMS IN LOCAL INFORMATION NETWORK

Головним недоліком існуючих методів і засобів захисту інформації, включаючи сучасні засоби пошуку вразливостей автоматизованих систем і виявлення несанкціонованих дій, є те, що вони, в більшості випадків організовують захист інформації лише від вже виявлених загроз, що показує певну ступінь пасивності захисту.

Одним з можливих напрямків вирішення проблеми захисту інформації в локальній інформаційній мережі від несанкціонованих дій є застосування методів обману. Такі системи отримали назву помилкових або обманних.

Механізм функціонування обманної системи полягає в тому, щоб залучити зловмисника в діалог з системою. При цьому обманні системи імітують уразливості реальних інформаційних систем. Зловмиснику доводиться постійно вирішувати: працює він з реальною системою або помилковою, витрачаючи при цьому ресурси.

Користувач який виконує всі інструкції, долає всі області з найменшими втратами часу. Порушник, намагаючись визначити вразливі місця в СЗІ, сканує поверхню пружного екрану, в результаті чого він або відбивається від екрану, або поглинається областями. Так як площі емулятора вразливостей значно більші, ніж реально існуючих, то порушник з великою ймовірністю потрапляє саме в "муляж". При цьому, до певного моменту часу порушник не підозрює, що працює з обманною системою. Намагаючись закріпитися в системі, і знайти слабке місце в наступному ступені захисту, він проявляє себе. У момент роботи обманної системи справжня система продовжує функціонувати і успішно вирішує покладені на неї завдання.

Застосування обманних систем захисту інформації в локальній інформаційній мережі дозволяє ввести в оману противника, збільшити час для прийняття необхідних заходів адміністратором і з деякою часткою ймовірності відвести загрозу від реальної працюючої інформаційної системи.

Література

1. Гладких А.А. Базові принципи інформаційної безпеки інформаційних систем. Ульяновськ 2012.
2. Пескова О.Ю. Використання обманних систем для захисту локальної мережі від зовнішніх загроз. М., 2013.